Public consultation on the contractual public-private partnership on cybersecurity and possible accompanying measures (EN)

General information on respondents

New Section

Please note that fields marked with * are mandatory.

Do you wish your contribution to be published?

Please indicate clearly if you do not wish your contribution to be published

X Yes

☐ No

Submissions that are sent anonymously will neither be published nor taken into account.

The Commission may contact you in case a clarification regarding your submission is needed depending on your reply to the following question.

Do you wish to be contacted?

X Yes

☐ No

I'm responding as:

☐ An individual in my personal capacity

x The representative of an organisation/company/institution

What is your nationality?

☐ Austria

☐ Belgium

☐ Bulgaria

☐ Croatia

☐ Cyprus

☐ Czech Republic

☐ Denmark

☐ Estonia

☐ Finland

☐ France

☐ Germany

☐ Greece

- Hungary
- Italy
- Ireland
- Latvia
- Lithuania
- Luxembourg
- Malta

x Netherlands

- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden
- United Kingdom
- Other

If you chose 'Other', please specify

Please tick the box that applies to your organisation and sector.

X National administration

- National regulator
- Regional authority
- Non-governmental organisation
- Small or medium-sized business
- Micro-business
- European-level representative platform or association
- National representative association
- Research body/academia
- Press
- Other

If you chose "Other" please specify

My institution/organisation/business operates in:

- [ ] All EU member states
- [ ] Austria
- [ ] Belgium
- [ ] Bulgaria
- [ ] Czech Republic
- [ ] Croatia
- [ ] Cyprus
- [ ] Denmark
- [ ] Estonia
- [ ] France
- [ ] Finland
- [ ] Germany
- [ ] Greece
- [ ] Hungary
- [ ] Italy
- [ ] Ireland
- [ ] Latvia
- [ ] Lithuania
- [ ] Luxembourg
- [ ] Malta

x Netherlands

- [ ] Poland
- [ ] Portugal
- [ ] Romania
- [ ] Spain
- [ ] Slovenia
- [ ] Slovakia
- [ ] Sweden
- [ ] United Kingdom
- [ ] Other

Please enter the name of your institution/organisation/business.

Rijksoverheid (Dutch National Government)

Please enter your name

N/A

Please enter the address of your institution/organisation/business

N/A

Please enter your telephone

N/A

Please enter your email

Contact information is sent separately to the Commission

What is your place of main establishment or the place of main establishment of the entity you represent (headquarters)?

The Hague, The Netherlands

Consultation

Note:

- *Depending on the question please make either one choice or multiple choices in responses to specific questions*
- *Please note that a character limit has been set for most open questions*

I. Identification of your priorities in cybersecurity

New Section

1. Which part of the value chain of cybersecurity services and products do you represent?

☐ Researcher
X Customer/User
☐ Supplier of cybersecurity products and/or services

X Public authority/government agency responsible for cybersecurity/research

If you answered "Researcher", please specify

If you answered "customer/user", which specifically?

☐ Certification/audit or standardisation agent
☐ Individual user
☐ SME user
☐ Private enterprise
X Public user
☐ Civil Society
☐ Other

If you answered "other", please specify

2. Which of the following describes the cybersecurity activities of your institution/organisation/business? (multiple answers possible)

2.1. Dedicated Cybersecurity -> Cybersecurity products/services

☐ Identity and access management
x Data security

X Applications security

X Infrastructure (network) security

☐ Hardware (device) security

x IT security audit, planning and advisory services

☐ IT security training

☐ Other

If you answered "other", please specify

2.2. Applied Cybersecurity -> Application areas with demand in cybersecurity products/services

X Critical infrastructures in general
x Energy
x Transport
x Health
x Finance and Banking
x Public Administration
x Smart Cities
x Digital Service Providers
x Protection of individual users
x Protection of SMEs

☐ Other

Please specify:

2.3. Applied Cybersecurity -> Specific IT technology areas with cybersecurity as a functional requirement
X Internet of Things
x Embedded Systems
x Cloud Computing
x 5G
x Big Data
x Smartphones
x Software Engineering
x Hardware Engineering

☐ Other

Please specify:

II. Assessment of cybersecurity risks and threats

New Section

1. Risk identification

1.1. What are the most pressing cybersecurity challenges for users (individuals, business, public sector)?

X Loss of know-how and confidential business information (trade secrets) – industrial and economic espionage, and other types of confidential information

X Industrial or economic sabotage (examples: disrupting or slowing down network and computer functioning)

☐ Extraction and use of identity and payment data to commit fraud

☐ Intrusion in privacy

x Other

Please specify:

For this, we refer to the outcomes of the most recent Cyber Security Assessment Netherlands (CSAN-2015, published October 2015)), which can be found at https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands.

The report concludes that the two first items already proposed in the questionnaire constitute the highest threat level in the Netherlands. To wit:

- Loss of know-how and confidential business information (trade secrets) – industrial and economic espionage, and other types of confidential information
- Industrial or economic sabotage (examples: disrupting or slowing down network and computer functioning)

Furthermore, theft and publication or selling of information mainly threatens private organizations and citizens. Takeover of IT (e.g. through ransomware) is primarily a threat to citizens. Disruption of IT is a concern for the government, private organizations and citizens alike.

Finally, digital espionage is a high threat to the government and private organizations.

1.2. Which sectors/areas are the most at risk? (please choose top 3-5)

X Critical infrastructures in general

x Energy

☐ Transport

☐ Health

x Finance and Banking

☐ Public Administration

☐ Smart Cities

x Digital Service Providers

☐ Protection of individual users

☐ Protection of SMEs

☐ Other

☐ I don't know

Please specify:

2. Preparedness

2.1. Are the necessary products/services available on the European market to ensure security of the whole value chain

- Yes
- x No
- I don't know

If no, which are missing - please provide examples:

No. In IT procurement, asymmetry exists between the security expertise of the vendor and the client, to the advantage of the vendor. Clients who lack security expertise have difficulty assessing the security posture of vendors, asking for additional functionality that would enhance security and weighing security benefits against costs.

The result is that IT vendors perceive a lack of interest from the market for investments in their products and services that would make clients more secure. So long as there is no effective way for a client to ensure that a vendor's product is more secure that the product of another vendor, it is more beneficial to a vendor to *say* his product is more secure than to actually make it so.

2.2. If relevant, where do the cybersecurity products/services you purchase come from?

- X National/domestic supplier
- European, non-domestic supplier
- US
- Israel
- Russia
- China
- Japan
- South Korea
- Other

If you answered "other", please specify

2.3. If relevant, what are the reasons behind your decision to choose non-European ICT security products/services over European ones?

☐ Price competitiveness

☐ Non-European products/services are more innovative

☐ Trustworthiness

☐ Interoperability of products/solutions

☐ Lack of European supply

☐ Place of origin is irrelevant

X Other

If you answered "other", please specify:

Tendering process

2.4. If relevant, what are the reasons for missing supplies of products/services in cybersecurity?

☐ Lack of capital for new products/services

x Lack of sufficient (national/European/global) demand to justify investment

☐ Lack of economics of scale for the envisaged (national/European/global) markets

☐ Market barriers

☐ Other

☐ I don't know

If you answered "other" please specify:

If in question 2.4. you marked "Market barriers", please specify:

☐ In the EU member state you operate

☐ Between EU member states

☐ Globally

☐ Between industry sectors

☐ Other

If you marked "other" please specify:

3. Impact

3.1. In which of the following areas would you expect the worst potential socio-economic damage? (please choose your top 1-5 answers)

X Critical infrastructures

X Energy

☐ Transport

☐ Health

X Finance and Banking

☐ Public Administration

☐ Smart Cities

X Digital Service Providers

☐ Protection of individual users

X Protection of enterprises (large companies and/or SMEs)

☐ Other

☐ I don't know

Please specify/explain

4. Cybersecurity challenges by 2020

4.1. What will be the 3 main cybersecurity challenges by 2020? (Please explain)

1. A main challenge will be to balance the need for increased cybersecurity with adequate protection of the privacy of individuals. Practical implementations of ‘privacy by design’ and ‘privacy by default’ are called for.
2. Vulnerabilities in software are still the Achilles heel of digital security. Although software vendors release security updates in large numbers, many organization do not install these updates due to a large number of reasons (e.g. incompatibility with existing legacy IT environments). A fundamental reconsideration of software design and maintenance practices (e.g. though ‘security by design’) is necessary to meet this threat.
3. Ever-increasing economic and national interests associated with proper functioning of internet-based services force the adoption of strict regulation of the internet as a ‘critical space’. This fundamentally undermines the open nature of the internet and, with it, its ability to facilitate speedy innovation and free participation.

III. Cybersecurity Market Conditions

IV. Need for public intervention and support for a functioning market in cybersecurity products/services in Europe

New Section

Please provide examples of successful support through public policies (at national or international level).

In 2011 the Dutch ICT Innovation Platform “Veilig Verbonden” (IIP-VV) released the first Dutch National Cyber Security Research Agenda (NCSRA). In 2013 an updated version of the agenda was published (NCSRA-II). Based on this agenda the Netherlands Organization of Scientific Research (NWO) and the Dutch government funded four cyber security calls for proposals (two calls in 2012 and two calls in 2013). NWO funded with their calls fundamental (scientific) research. The Dutch government funded with their calls Small Business Innovative Research (SBIR) projects. The four calls have resulted in a large number of relevant research projects and prototypes of innovative cyber security products. Next to the calls, several cyber security research & innovation events were organized by NWO and the Dutch government (e.g. NCSRA-symposia, matchmaking days).

In November 2015, Dick Schoof, National Coordinator for Security and Counterterrorism of the Dutch Ministry of Security and Justice, officially announced the launch of a new platform for Cyber Security Research & Education (CSRE). Main objective of the new platform is to maintain and intensify the connections between the stakeholders in the cybersecurity domain and knowledge chain. The CSRE Platform is mentioned the Dutch Cyber Security Strategy (NCSS2) as an important means to fulfil the goal to guarantee the necessary knowledge, skills and innovation in cybersecurity. In this platform start-ups, established companies, students and researchers can connect, inspire one another and attune research supply and demand. Establishing agenda’s for cybersecurity research & innovation and organizing research & innovation events will be two of the tasks of the platform. The actual launch of the platform will take place in 2016.

V. Specific Industrial Measures

New Section

The first question in this section complements the overall public consultation on the Priority ICT Standards Plan with respect to the specific characteristics of cybersecurity standardisation. We understand by standardisation in this context the production of technical specifications, standards or architectures where there is a need/gap, but also any other type of standardisation action such as landscape analysis, gap finding, roadmaps or ecosystem building.

1. How would you evaluate the current role of standardisation in the domain of cybersecurity?

1.1. Have you applied or are you currently working with specific technical specifications, standards or architectures relevant to cybersecurity?

The Dutch government has implemented an open standards policy for the public

sector. The most visible component is the ‘Comply or Explain’ list of open standards, mandatory for governmental organizations. This list contains several standards/TS that are relevant for (cyber)security: DKIM, DNSSEC. SPF, TLS, ISO/IEC27001 + 2.

Government agencies are bound to follow certain ICT security standards, and to require them in procurement of ICT products/systems. For the market side: there is no regulation in which specific standards are required. The development and usage of internet standards is being promoted and encouraged, in particular regarding cybersecurity. We encourgae the use of internet standards and software security standards.

1.2. In what areas is there a need/gap in this respect?

The gap problem is mainly the lack of adoption and implementation of existing standards. Promotion of good practices including the latest standards therefore should have high priority. Warding off and preventing incidents has proven to be an effective approach, which asks for considerable effort, though. It requires to create per sector or chain a setting of trust and confidentiality involving representatives of industry as well as government (ISAC).

Furthermore is needed:

- guidance on security and privacy by design, that goes beyond theoretical constructs to facilitate and enhance implementation.
- Process standard for cyber risk management: unclarity of terms and definitions hampers the effective and efficient cooperation between European stakeholders.This is exacerbated by the continued growing integration of production and service processes, for which end-to-end security assurance is becoming indispensable.
- Secure Internet Standards: up to date, secure internet standards are often implemented too late or not at all. Maximum effort on broad deployment of secure, future-proof internet technology is needed.
- Standards for authentication and authorisation: eIDAS regulation is a meaningful initiative for access and access control, yet unambiguous choices for standards as well as ongoing development of existing specifications are needed

1.3. Would you consider standardisation as a mean to support innovation and the digital single market in cybersecurity?

X Yes

☐ No

☐ I don't know

Please explain your view

The right kind of standardisation drives innovation, e.g. because SMEs don’t have to reinvent the wheel regarding security issues. Knowledge and standardization are key elements regarding SDSM and the international digital agenda’s.

Technical standards for security and privacy by design

Security and privacy by design are expected to be key elements of the upcoming Data Protection Regulation. In the light of the compulsory character of the regulation, guidance on these issues that go beyond theoretical constructs will aid stakeholders in the European marketplace in bolstering their competitive position. Technical standards will make the targets of European industry tangible and comparable, thus aiding market transparency.

Also, consumers will be able to assess the compliance of products with the latest regulatory requirements.

Process standard for cyber risk management

Cyber risk management is a rapidly emerging aspect of generic risk management. Stakeholders will benefit from practical guidance. A process standard for cyber risk management is expected to facilitate supply chain integration.

Secure Internet Standards

The Internet has become indispensable in all aspects of society. It is of major importance to foster a secure internet. For individuals as well as public and private parties, confidence in the trustworthiness of the internet is very important.

Standards for authentication and authorisation

eInteraction/ eServices / eDelivery all need trust. Businesses as well as citizens benefit from proper authentication and authorisation structures and mechanisms.

1.4. Should standardisation in cybersecurity be addressed generically or should it focus on specific sectors (e.g. transport, energy, finance) and areas of application (e.g. connected vehicles, smart-grids, electronic payments)? (Please specify your choice)

Both sector wide and sector specific standardization have their merits.

1.5. What areas should future cybersecurity standardisation efforts focus on? (Please specify).

As said before; there is less a need to develop new standards, as there is a need to adopt and implement standards. That said more can be done in at the front end side of product development: secure software development, hardware, security by design.

2. Assessment of existing certification schemes in the field of cybersecurity

2.1. Are you active in public or private certification bodies?

☐ Yes
X No

If yes, please specify:

2.2. Which existing ICT security certification schemes would you consider successful and what learnings should be taken from them for future cybersecurity certification activities?

ISO/IEC 27001 & 2

At boardroom level there is a lack of awareness regarding international ICT standards and standards for vital infrastructures and the importance of issues like security and privacy is often overlooked at that level. In this regard there is an enormous gap between the operational and strategic levels within companies or holdings. Those in charge are

unconsciously incompetent in trhat area and are not being supplied with clear information and lines to take.

The reference framework for secure software still is under development. Certification is not an goal in itself; it can only be effective in a more mature market which offers sufficient incentives for differentiation (quality).

2.3. Do the current ICT security certification schemes adequately support the needs of European industry (either supplying or buying cybersecurity solutions)?

- Yes
- No
- X I don't know

Please explain

2.4. How relevant are certification schemes to the digital single market in cybersecurity products and services?

Provided they are developed the right way, certification can reassure customers and clients. Certification for its own sake has little use and is frowned upon by SMEs as a cash cow. This would not benefit innovation, in particular in those case where SMEs are obliged to make substantial investments to obtain or keep certain certificates.

2.5. What areas should future certification efforts focus on?

Critical areas / infrastructures

2.6. Are certification schemes mutually recognised widely across European Union's Member States?

- Yes
- No
- X I don't know

Please specify

ISO/IEC 27001 & 2 might be an example in case.

2.7. Is it easy to demonstrate equivalence between standards, certification schemes, and labels?

- Yes
- X No
- I don't know

Please explain

For standards and certificates, see above. As regards labels we only see limited added value. Food industry is a case in point, where so many labels are being used that consumers can't establish their meaning and value. To industry they can be a burden.

3. Are you aware of any existing labelling schemes for cybersecurity products and services in Europe or in the rest of the world?

☐ Yes
X No

3.1. If yes, please specify if you are referring to legal labelling schemes or industry self-labelling schemes.

3.2. If yes, how do you assess the efficiency of such labels to provide visibility and readability for buyers?

3.3. How would you assess the need to develop new or expand existing labels in Europe?

3.4. Which market(s) would most benefit from cybersecurity labels?
X Consumer market
X Professional market (SMEs)
☐ Professional market (large companies)
☐ I don't know

3.5. What criteria / specific requirements are necessary to make such labels trustworthy?

4. What form of access to finance would be most useful for European cybersecurity industry players to encourage business growth?

☐ Bank loans
☐ Equity funds
☐ Venture funds
☐ EIB/EIF support
☐ Sovereign welfare funds
X Crowdfunding
X EU funds, please specify
☐ Other

Please explain

5. What specific start-up policy measures do you consider useful for the cybersecurity industry in the European Union?

6. What do you think would be the right measures to support the EU market access and export strategy for cybersecurity products and services?

Europe should investigate a harmonised EU certification of security of ICT products, similar to CENELEC as concerns the safety of products. Furthermore Europe should promote

- ‘security by design’
- compulsory transparancy regarding responsibilities / accountability / liability throughout the chain

VI. The role of research and innovation in cybersecurity

New Section

1. Have you participated in previous R&I efforts through European (FP7, CIP) programmes?

2. On which levels would you focus public support for research & innovation measures (please identify in % - total should be equal to 100%)?

	% (specify 0-5-10-15-25-50-100)
Fundamental research	20
Innovation activities	20
Using research & innovation results to bring products and services to the market	5
Development of national/regional cluster (or national/regional centres of excellence)	5
Start-up support	5
SME support	5
Public Procurement of innovation or pre-commercial support of development and innovation	20
Individual, large-scale "Flagship" initiatives	0
Coordination of European innovation and research activities	10
Definition of common requirements for cybersecurity products and services for specific application domains at European level (e.g. transport, energy…)	10
Other (please specify)	0
TOTAL (100%)	100

3. In which areas would a prioritisation of European support actions be most effective? (Please identify your 3-5 top priorities)

3.1. In terms of research priorities following the terminology of the Strategic Research Agenda of the NIS Platform [1]
X Individuals' Digital Rights and Capabilities (individual layer)
X Resilient Digital Civilisation (collective layer)
X Trustworthy (Hyperconnected) Infrastructures (infrastructure layer)

☐ Other

Please specify:

3.2. In terms of products and services
X Identity and access management

☐ Data security
X Applications security
X Infrastructure (network) security

☐ Hardware (device) security

☐ IT security audit, planning and advisory services

☐ IT security management and operation services

☐ IT security training

☐ Other

Please explain:

Identity and access management: we need research in novel access management techniques to help regulate who gets access to what information and under what circumstances. Given the current trend toward storing more and more data into the cloud, with the associated ambiguities regarding ownership and access, this problem is increasingly important.

Applications security: existing and new applications. Most exploits still focus on PHP applications and applications on Windows platforms. Security often has no priority in the development of new applications.

Infrastructure (network) security: especially attack detection & prevention. To detect and prevent attacks, we need techniques and tools to spot and remove vulnerabilities from software, and monitoring systems to raise an alarm when a system behaves in an anomalous manner. Likewise, compliance monitoring is important to spot vulnerabilities (in systems and organisations) as early as possible.

4. In which sectors would a prioritisation of European support actions be most effective? (Please identify top 3 to 5 and explain)
X Critical infrastructure in general

☐ Energy
X Transport

☐ Health
X Finance and Banking

☐ Digital Service Providers

X Internet of Things

☐ Cloud Computing

☐ Public Administration

☐ Other

Please explain your choice:

Critical infrastructure in general: especially Industrial Control Systems (ICS). Chemical and nuclear plants, and large parts of the national critical infrastructure, such as the water, gas and electricity supply are monitored and controlled by ICS. Disruptions in ICS can have disastrous consequences, but their increasing reliance on ICT – including the Internet – has made them vulnerable to remote attacks.

Transport: cars and transportation systems are increasingly making use of sophisticated software to carry out safety-critical processes (such as braking in cars). In aviation, passengers are more and more often allowed to use their own devices during flights. Several carriers already offer wireless internet facilities to their passengers. Of course, these networks must remain separate from the aircraft control system.

Finance and Banking: financial institutions or their customers are increasingly often victim of targeted cyber attacks, carried out by well-funded criminal organisations, that are becoming ever more sophisticated.

Internet of Things: including medical devices. In coming years an increasing number of household appliances, medical and industrial equipment will contain all sorts of sensors. They will continuously exchange data via an internet connection. The developments are still in their infancy, but will most certainly have an impact on cyber security: devices that are online run risks and are potentially vulnerable.

5. In your opinion which bodies merit particular attention? (Please explain for each category you select)

X Universities and Research Institutes

X SMEs

X Start-ups

☐ Enterprises with large market share in nation markets ("National Champions")

☐ Enterprises with strong positions on global markets ("Global players")

☐ Other

Please explain:

Cyber security research spans a broad range from short-term to long-term, and from applied to fundamental. At one end of the spectrum are short-term consultancy-type projects, e.g. to evaluate security concerns or proposed solutions. Because of their urgent and ad-hoc nature, these do not easily lend themselves to synchronization in a broader research program. At the other end of the spectrum is fundamental scientific research, carried out at universities and research institutes. Intermediate forms are carried out inside and across

many companies and organizations. It is important to allow Universities and Research Institutes, SMEs and Start-ups to conduct the broad range of research. Enterprises with large market share in nation markets ("National Champions") & Enterprises with strong positions on global markets ("Global players") have the funds to invest in research & innovation themselves.

6. What are the specific needs of innovative SMEs in cybersecurity to stimulate competitiveness? What specific type of public support would be most useful to such companies?

Clear view on the market: a place where people can connect, inspire one another and attune research & innovation supply and demand.
Co-funding.
Minimal administrative burdens.

7. What would be your contribution to fostering innovation and competitiveness of cybersecurity in Europe?
X Support in alignment of national and European research agendas
X Support for SMEs
X Co-funding of national or European activities
X Providing infrastructures for experimenting and testing
X Support with expertise in standardisation bodies
X Contribute to certification schemes
☐ Other

Please explain

With our (earlier mentioned) CSRE Platform, we will be able to contribute to supporting the alignment of national and European research agendas, supporting SMEs, co-funding of national or European activities, and providing infrastructures for experimenting and testing. Support with expertise in standardisation bodies and contribute to certification schemes are already part of our activities.

VII. The NIS Platform

New Section

This section is a separate part of the consultation, not related to the cPPP and accompanying measures, but looking for interested stakeholders' views on the public-private network and information security Platform (NISP).

The NIS Platform, which was one of the actions under the EU Cybersecurity Strategy, was established in June 2013. Its aim was to identify good cybersecurity practices that organisations can implement in order to increase their resilience. These practices were expected to facilitate the future implementation of the NIS Directive, but are also relevant to a wide range of organisations not covered by the Directive.

The Platform gathered almost 600 stakeholders representing the business community, civil society, academia, researchers and member states. NIS Platform work has been divided into three sub-groups dealing with risk management; voluntary information exchange and incident coordination as well as secure ICT research and innovation. Over the course of two years

the working groups have developed a number of deliverables, including the Strategic Research Agenda, which feeds into the process of creating the contractual Private Public Partnership on cybersecurity addressed in the previous sections of this consultation.

The Commission would like to take the opportunity to ask stakeholders, who participated in the efforts of the NIS Platform, about their views on Platform's work to date. The Commission would also like to have the views of all interested stakeholders on the future of the NIS Platform. It will take these views into consideration in the process of developing a new Work Programme for the NIS Platform following the expected adoption of the NIS Directive in early 2016.

1. NIS Platform format - what did you like about the structure and working methods of the NIS Platform and what would you suggest changing (if anything)?

Question for stakeholders who took part in the NIS Platform's work

The structure of the NISP with working groups focussing on specific topics is good. There are, of course, improvements possible. The main focus should lie on three elements: transparency, a broad base of support and value for time investment.

<u>Topics</u>: The way topics of the working groups are selected is unclear. It seems to be a combination of EC views and selected ideas from the NISP community.

<u>Process</u>: The process of how certain recommendations are concluded by the working groups should be more transparent. Also a way should be devised how the NISP plenary can validate these findings. Also it is now quite time consuming to add to the findings of the working groups. Sending in papers or opinions are always subject to review by individuals with their own views (maybe even agenda's). In order to ensure important viewpoints to survive the working group process requires a hefty time investment which not every organisation can afford.

<u>Adopting findings</u>: It should be clear how the findings of the working groups are adopted by either the EC or by other fora/in other processes.

2. What possible future areas of work should the NIS Platform focus on following the adoption of the NIS Directive?

Question for all stakeholders

New topics worthy of exploration are:

- How do we ensure that the NISD incident reporting scheme is going to add value to the broader cyber security community?

- The importance of SME's, the value chain, and sectoral/chain dependencies is growing. Best practises in how to deal with these challenges would be very welcome.

Depending on the final form the Cooperation Group will take a possible role for the NIS Platform could be in:

- exchange information and best practices in the fields of awareness raising and training

- Exchange information and and best practices: research and development on network and information security

3. What were your reasons for engaging/not engaging in the NIS Platform's work so far?

Question for all stakeholders

The Netherlands believes in public-private cooperation as one of the solutions in increasing cyber security. The NISP is one of the few public-private partnership networks on a

European level. It is important to provide the EC with a broad range of views, both from private companies as national public entities involved in cyber security.

4. What would be your motivation for engaging in the NIS Platform's work after the adoption of the NIS Directive, and what expectations would you have?

Question for all stakeholders

The NIS Platform could develop advises to the member states in how to identify operators of essential services, together with ENISA.

(see also the answer to 3 above)

VIII. Sharing your data and views

New Section

Please upload additional data and information relevant to this survey.

[1] For further information, please consult the Strategic Research Agenda of the WG3 Network and Information Security (NIS) Platform - https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/strategic-research-agenda-draft-v02.63/view